

HR 2481: PROTECTING OUR ABILITY TO COUNTER HACKING (PATCH) ACT OF 2017

House Sponsors

Lieu (D-CA)
Farenthold (R-TX)

Senate Sponsors

Schatz (D-HI) Johnson (R-WI)
Gardner (R-CO)

"Building up a huge stockpile of undisclosed vulnerabilities while leaving the Internet vulnerable and the American people unprotected would not be in our national security interest."

**– Michael Daniel, White House
Cybersecurity Coordinator (2014)**

THE BACKGROUND

When the government discovers a vulnerability in technology products, applications and systems, it must decide whether to retain the vulnerability for offensive use or disclose it to vendors for defensive hardening. In 2010, the Executive Branch set up a working group to oversee this Vulnerabilities Equities Process (VEP). [CRS Memo](#).

THE PROBLEM

The government's current decision-making process for whether to retain or disclose cyber vulnerabilities is opaque, unaccountable to Congress, and unestablished in law or Executive Order. That undermines trust with the American people and private sector and potentially jeopardizes our nation's cybersecurity.

THE SOLUTION

The PATCH Act codifies current government practices, adds oversight mechanisms, and gives the Executive Branch the flexibility to strike an appropriate balance between intelligence needs and cybersecurity responsibilities regarding vulnerability disclosure.

Outside Support:

Coalition for Cybersecurity Policy
and Law | McAfee | Mozilla |
Information Technology and
Innovation Foundation |
R Street Institute | Center for
Democracy and Technology |
New America's Open
Technology Institute

If you have any questions or wish to cosponsor, please contact:

Corey Jacobson (Lieu)
corey.jacobson@mail.house.gov
Alyssa Wootton (Farenthold)
alyssa.wootton@mail.house.gov

WHY CODIFY THE VULNERABILITIES EQUITIES PROCESS (VEP)?

- Balance two national security interests: the need to collect actionable intelligence & the need to patch vulnerabilities in technology products used by U.S. consumers and businesses
- Bring transparency to the process by making public the aggregate number of zero day vulnerabilities discovered and disclosed, and the average time before disclosure. This added transparency will not apply to details of vulnerabilities or agency activities.
- Allow Congress to conduct better oversight over the government's decision-making on retaining and disclosing vulnerabilities
- Ensure continuation of the VEP from Administration to Administration